АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

UDC 004:005.21:005.334

DOI https://doi.org/10.5281/zenodo.20668246

The limits of automation and the role of the human factor in making emergency IT decisions

Revenko Olena,
PhD in Economics, Associate Professor,
Associate Professor of Enterprise Economics and Business Organization Department,
Simon Kuznets Kharkiv National University of Economics,
Nauky Avenue, 9A, Kharkiv, Kharkiv region, 61166,
https://orcid.org/0000-0003-0110-7291

Khvostikov Andrii,
PhD in Economics,
Lecturer at the Department of Enterprise Economics and Business Organization,
Simon Kuznets Kharkiv National University of Economics,
Nauky Avenue, 9A, Kharkiv, Kharkiv region, 61166,
https://orcid.org/0000-0003-1177-9761

Accepted: 18.05.2026 | Published: 30.05.2026

Abstract. In the context of emergency decision-making in IT companies, automation does not eliminate risks but transforms them, increasing the likelihood of rare but critical failures. Despite the effectiveness of artificial intelligence systems in performing routine operations, it is humans who remain the key element in stabilizing the system in conditions of uncertainty and non-standard situations.

The study focused on the concepts of automation bias and human models in the adaptive control circuit. It was found that cognitive factors affect the quality of decision-making in critical situations when standard algorithms encounter uncertainty. This is of particular importance in incident management and cyber defense processes, where decisions must be made quickly and in conditions of information scarcity.

The levels of automation and human involvement were analyzed, with the most common management risks in mind. The specifics of the application and the effectiveness of Human-SRE and AI-SRE were also analyzed. Effective practical approaches to minimizing the negative impact of automation and maximizing human potential in the IT sphere are proposed.

It has been shown that excessive reliance on automation can lead to cognitive degradation among personnel, loss of critical-thinking skills, and reduced situational awareness. In this regard, IT companies should invest not only in digital technologies but also in developing employees' autonomous response skills. An important condition for security is ensuring the transparency of algorithms and personal responsibility for emergency decisions. Ukrainian experience of IT companies operating in wartime demonstrates the effectiveness of combining a high level of automation with the adaptability of human capital. It is the balance between technological support and human control that underpins the stability of emergency management systems in the modern digital environment.

The domestic IT sector's experience during the war demonstrates the effectiveness of the human-centric automation model. The stability of emergency management systems is based on preserving a person's role as an active and autonomous subject. In this paradigm, digital tools do not replace human capital but expand human capital's adaptive capabilities, which is critical to system stability in a dynamic digital environment.

Keywords: adaptive management, personnel, hybrid employment, information technology, experience, IT sphere, emergency solutions, interaction, cognitive load, uncertainty, automation strategy.

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Межі автоматизації та роль людського фактора під час ухвалення екстрених рішень у сфері IT

Ревенко Олена Вікторівна,
кандидат економічних наук, доцент,
доцент кафедри економіки підприємства та організації бізнесу,
Харківський національний економічний університет імені Семена Кузнеця,
проспект Науки, 9А, Харків, Харківська область, 61166,
https://orcid.org/0000-0003-0110-7291

Хвостіков Андрій Ігоревич,
доктор філософії з економіки,
викладач кафедри економіки підприємства та організації бізнесу.
Харківський національний економічний університет імені Семена Кузнеця.
проспект Науки, 9А, Харків, Харківська область, 61166,
https://orcid.org/0000-0003-1177-9761

Анотація. В умовах забезпечення ухвалення екстрених рішень в IT-компаніях автоматизація не усуває ризики, а трансформує їх, створюючи ймовірність рідкісних, але критичних збоїв. Попри ефективність систем штучного інтелекту у виконанні рутинних операцій, саме людина залишається ключовим елементом стабілізації системи в умовах невизначеності та нестандартних ситуацій.

В дослідженні увага була зосереджена на концепціях упередженості автоматизації та моделях людини в контурі адаптивного управління. З'ясовано, як саме когнітивні аспекти впливають на якість ухвалення рішень у критичних ситуаціях, коли стандартні алгоритми стикаються з невизначеністю. Особливого значення це набуває у процесах інцидент-менеджменту та кіберзахисту, де рішення необхідно приймати оперативно та в умовах дефіциту інформації.

Було проаналізовано рівні автоматизації та залучення людини з урахуванням найбільш поширених ризиків у сфері управління. Також проаналізовано специфіку застосування та ефективність Human-SRE й AI-SRE. Запропоновано дієві практичні підходи до мінімізації негативного впливу автоматизації та максимізації людського потенціалу в ІТ-сфері.

Доведено, що надмірне покладання на автоматизацію може призводити до когнітивної деградації персоналу, втрати навичок критичного мислення та зниження ситуаційної обізнаності. У зв'язку з цим ІТ-компанії повинні інвестувати не лише у цифрові технології, а й у розвиток навичок автономного реагування працівників. Важливою умовою безпеки є забезпечення прозорості алгоритмів та персональної відповідальності за вжиті екстрені рішення. Український досвід функціонування ІТ-компаній в умовах війни демонструє ефективність поєднання високого рівня автоматизації з адаптивністю людського капіталу. Саме баланс між технологічною підтримкою та людським контролем формує основу стійкості систем екстреного управління в сучасному цифровому середовищі.

Досвід функціонування вітчизняного ІТ-сектору під час війни демонструє ефективність людиноцентричної моделі автоматизації. Стійкість систем екстреного управління базується на збереженні за людиною ролі активного та автономного суб'єкта. У цій парадигмі цифрові інструменти не заміщують людський капітал, а розширюють його адаптивні можливості, що є критично важливим для стабільності систем у динамічному цифровому середовищі.

Ключові слова: адаптивне управління, персонал, гібридна зайнятість, інформаційні технології, досвід, ІТ-сфера, екстрені рішення, взаємодія, когнітивне навантаження, невизначеність, стратегія автоматизації.

Problem statement. The modern information technology ecosystem is highly complex, with interactions among distributed systems, cloud computing, and artificial intelligence (AI) algorithms occurring at speeds beyond human perception. In this

context, automation has ceased to be just an auxiliary tool and has become a fundamental condition for the existence of digital infrastructure. However, despite technological progress, the occurrence of critical incidents and states of high uncertainty remain an integral part of the operation of any complex system. It is at such moments that the limits of automation become most obvious, and the role of the human factor is perceived as decisive for the survival of business and data security in general.

The problem with the limits of automation lies not only in the technical limitations of algorithms but also in the sociotechnical paradox: the more advanced an automated system becomes, the more complex and critical the tasks remaining for the human operator become. In conditions of uncertainty, when inputs can be imprecise and heterogeneous, and the context of the incident is unique, deterministic algorithms often fail, requiring humans to coordinate adaptively and even engage in heuristic thinking. Recent years have seen the rapid implementation of "agent-based" artificial intelligence and AI-SRE (site reliability engineering) systems, which promise the autonomous elimination of failures. However, practice suggests otherwise, as the number of incidents related to AI misoperation or misinterpretation is increasing, which actualizes research on cognitive traps such as automation bias.

For Ukraine, these issues acquire a special dimension. The constant cyber threat, energy instability, and hostilities create an environment of extreme uncertainty, in which IT professionals are forced to make decisions under high cognitive load and physical danger. In such circumstances, automation should not only speed up processes but also maintain the specialist's mental stability by providing transparent and explainable recommendations. This report offers an in-depth analysis of the mechanisms underlying human interaction and automation, based on modern scientific research and empirical data from major IT incidents over the last five years.

Analysis of recent research and publications. The analysis of the mechanisms of interaction between technologies and humans in management processes was considered by many researchers, including such researchers as N. Amalia, B. Tiagiono, V. Palade [1], L. Bainbridge [2], T. Wentworth [3], J. Kincl, M. Adam, T. Pavleska [5],

J. D. Lee, B. Seppelt [6], G. Lopushniak, O. Poplavska, N. Danylevych, T. Kostyshyna, R. Raupov [7], K. Ozarko, M. Pikh [9], R. Parasuraman, R. Riley [13], B. Strauch [14] and others.

The study of human interaction with automated systems has a long genealogy, the roots of which go back to the work of L. Bainbridge [2], who was the first to prove that automation does not eliminate human errors, but only moves them from the operational level to the level of system design and configuration. She identified five main "ironies", among which the most important for IT is the degradation of the operator's skills, who, due to constant observation, loses the ability to intervene manually at critical moments. Over time, such ideas were continued in the works of K. Trim [11] and B. Strauch [14].

The development of this topic in the 90s is associated with R. Parasuraman and R. Riley [13], who proposed a four-stage model of automation: information collection, information analysis, action selection, and action execution. Their contribution consists of formulating the concepts of excessive trust, ignoring due to frequent false alarms, and automating functions without accounting for the human factor. These works laid the foundation for the modern understanding of trust in front-end automation of business processes.

In recent years, starting with the Covid-19 pandemic, scientific discourse has shifted towards AI and complex adaptive systems, driven by the spread of hybrid forms of employment. John D. Lee [6] emphasizes the need to move from "technocentric" to "human-centric" design, focusing on a joint "human-automation" system. A significant contribution to the study of cognitive aspects during this period was made by researchers J. Kinzl, M. Adam, T. Pavleska [5], who systematized the risk groups of artificial intelligence, highlighting the problems of system security and reliability as priorities.

The Ukrainian Scientific School is actively working on the topic in the context of national sustainability. The works of K. Ozark and M. Pikh [9] focus on the managerial aspects of the IT sector in the context of international integration, in which

the human factor is considered an indicator of enterprise security. The socio-behavioral nature of risks in database security has been studied in detail by experts [1, 4, 7], who emphasize that technical vulnerabilities often stem from cognitive overload and personnel stress. Methods for automating decision-making under uncertainty were also developed, particularly through intelligent systems for analyzing big data.

Modern empirical studies by organizations such as IBM and Palo Alto Networks, as well as systematic reviews in MDPI and Frontiers journals, confirm that despite automation, 95% of successful cyberattacks remain attributable to human factors [5], indicating a gap between technological potential and the operational readiness of personnel. Practices have also shown that if the team's productivity increased by 40% but their ability to detect minor errors decreased by 20%, the company did not gain a net benefit [11].

Formulation of the objectives of the article (statement of the task). The purpose of the study was to conceptualize the limits of automation in the modern IT sphere, to substantiate the critical role of the human factor in decision-making processes during emergency situations under conditions of uncertainty, and to identify practical models for building resilient systems in which automation enhances rather than replaces human expertise.

Presentation of the main material of the study with full justification of the scientific results obtained. The idea of full automation rests on the assumption that digital systems are completely deterministic. However, the reality of IT infrastructure is the formation of a state of "fluid complexity", where interactions between components give rise to emergent properties that cannot be predicted at the stage of writing code. The limits of automation lie where the known logic ends and the unknown begins, so automation, of course, is not a panacea.

Bainbridge L. [2] pointed out that automation designers are human themselves and tend to carry their errors into algorithms. This creates the first "irony", i.e. we automate tasks because humans are unreliable, but we create automation with the help of the same unreliable people. It faces the risk of AI generating syntactically correct

but logically destructive code. Table 1 analyzes the levels of automation and human involvement, with consideration of the most common risks.

At higher levels of automation, a certain paradox of supervision arises. Practice shows that a person must control a system that works much faster than they do and intervene exactly when the system can no longer cope. This means that a higher level of skill is required of the operator to handle the most complex cases, although in his daily work, he lacks the practice to maintain these skills.

Table 1. Comparison of Levels of Automation and Human Engagement (Parasuraman-Sheridan Model)

Level	Level description	The role of man	Main risks
1-2	Low (manual)	Full control, AI only collects data	High fatigue, low speed
3-5	Medium (support)	Chooses from the options offered by AI	Cognitive overload when choosing
6-8	High (supervision)	Intervenes only in case of refusal, AI acts autonomously	Automation bias, loss of skills
9-10	Full (autonomy)	Missing or ignored	Complete loss of situational awareness

Source: formed by the author according to [1, 10, 13]

From a strategic point of view, I wonder what happens within decision-making processes under extreme conditions? Emergency decisions in IT are usually justified in conditions of time shortage, high cost of error, and information noise. In such states, the human psyche enters a mode of rapid thinking, making the specialist vulnerable to cognitive distortions. Then it is the automation bias that describes the phenomenon in which a person tends to trust the conclusions of an automated system more than their own feelings or alternative sources of information. During IT incidents, engineers often ignore abnormal monitoring metrics when the smart control panel glows green. Studies show that even experienced pressure professionals tend to hit the approval button on an AI agent's recommendations without checking their essence, just to complete an incident faster.

To make a successful decision, an engineer must not only see the data but also understand its connections and predict the future, thereby being situationally aware. Automation often "blinds" the operator, providing him only with results, not the process of obtaining them. When the AI system says "overload the server" without explaining why, the operator loses touch with the actual state of the infrastructure.

For Ukrainian IT teams, uncertainty is compounded by stress from external threats. Studies from the beginning of the war [7] show that 30% of Ukrainian researchers and engineers work remotely with unstable access to the grid and electricity. This creates unstable working conditions because the engineer must make a critical decision about a database migration during an air raid. Under such conditions, cognitive resources are depleted much faster, making automation (for example, autopilots in Kubernetes) critical yet dangerous due to the impossibility of full supervision.

To maintain the system's operability under uncertainty, it is necessary to implement the HAIF strategy, which establishes a protocol requiring that any autonomous AI action have a clear "trace" and the possibility of instant rollback by a person (Table 2). These simple steps effectively counteract the degradation of staff skills.

Table 2

Human-SRE and AI-SRE Performance Comparison

Showman	Human-SRE	AI-SRE	Features of manifestation
Log analysis speed	Minutes, hours	Seconds	AI wins at high volumes
Understanding the nuances of business	Tall	Low	People know why the service is critical
Responsibility	Full	Absent	People have an ethical responsibility
Elimination of "black swans"	Adaptive	Weak	AI is based on experience

Source: summarized by [4, 3, 8]

So, it should be emphasized that the limit of automation is not only a technical error, but also a loss of controllability. Implementing a leader with the highest level of AI oversight in today's realities is necessary to avoid diluting responsibility when the

organization blames the algorithm for a false emergency decision. The data show that the greatest damage is caused by incidents in which a person acts either as an object of manipulation (social engineering) or as a source of unintentional errors in complex configurations that automation cannot verify.

It should be noted that the country of location and the business's market presence also exert a determining influence. Recently, the specificity of Ukraine has been that decision-making can take place amid total uncertainty. Today, the Ukrainian IT sector is a unique testing ground for exploring the limits of automation. The uncertainty here is not only technical, but also physical. Regular power outages necessitate automating load migration between data centers. However, the decision on whether to keep the system "alive" during shelling, with staff in storage facilities, is both ethical and strategic and reflects infrastructural instability. It is worth addressing psychological stability as a security factor. Studies [9, 12] show that the level of cyber hygiene in Ukrainian companies correlates with the team's psychological state. In the face of chronic stress, automation bias increases, which means that people tend to delegate complex decisions to the machine to reduce their own anxiety. It is also important to implement adaptive management tools in practice. Ukrainian companies (for example, in the fintech sector) are implementing dynamic roles in which responsibility for emergency decisions is distributed based on team members' situational awareness in safe areas.

Thus, to minimize the negative impact of automation and maximize human potential, the following approaches can be effective:

1. The design is for inspection, not approval. Instead of "approve/reject" interfaces, which usually train the habit of agreement, systems should be used that require a person to make a prediction or answer questions about AI logic before performing an action. Essentially, it supports cognitive engagement.

2. Preservation of manual paths. Organizations must conduct periodic "manual control" days when critical operations are performed without the help of AI agents. This helps you combat skill loss and ensures that, in the event of a complete automation

failure, the team can restore the system from "bare iron". The biggest risk is that, without understanding the logic behind how artificial intelligence models operate, the operator cannot exercise full control over the decision-making process, turning automation into a "black box" with unpredictable consequences.

3. Practice of the stress vaccination method. Through simulation exercises, teams should be gradually exposed to scenarios in which automation provides incorrect advice. This fosters a "healthy distrust" and teaches specialists to recognize moments when the system exceeds its competence. So, in the realities of Ukraine, this method helps not to avoid stress, but to teach the psyche to digest it correctly.

Conclusions. The study of the limits of automation and the role of the human factor in IT allows us to assert that we are at the stage of a paradigm shift: from attempts to replace a person to attempts to expand his capabilities through the complementarity of man and machine. The importance of modern enterprises in the IT sector in resolving the contradiction between the desire for full process automation and the irreplaceability of human intuition amid high uncertainty has been demonstrated.

In the context of ensuring emergency decision-making in IT companies, automation is increasingly not a tool for the complete elimination of risks, but a mechanism for their transformation. The use of complex systems based on artificial intelligence reduces routine errors and speeds incident response, but also creates conditions for rare yet critical failures that can cause large-scale consequences for digital infrastructure. In such situations, the person remains the key element in system stabilization, since algorithmic models cannot fully account for unpredictable contexts, ethical dilemmas, or non-standard scenarios in the unfolding of events. This is especially important in the processes of incident management, cyber protection, and business continuity, where decisions must be made under high uncertainty and time pressure.

At the same time, excessive dependence on automated solutions poses a risk of cognitive degradation among operators and IT specialists, who gradually lose the skills of independent situational analysis, critical thinking, and working without digital

prompts. This poses an additional threat to organizational resilience, since when automated systems fail, personnel may not be ready to respond promptly. That is why modern IT companies should invest not only in technological updates but also in developing employees' competencies, particularly by modeling crisis scenarios, training for offline work, and developing skills for quick decision-making in critical situations.

The basic condition for the effective functioning of emergency decision support systems is also to ensure the transparency of algorithms and clear personal responsibility for their application. In this conceptual context, the implementation of the HAIF strategy serves as a guarantor of the security of digital systems, since it allows the combination of the speed of algorithmic analysis with human responsibility and ethical control.

Of value for global practice is the Ukrainian experience of IT companies operating in wartime, which demonstrates the effectiveness of combining a high level of automation with maximum adaptability of human capital. Ukrainian IT specialists prove that the most sustainable management model is one in which a person is not removed from the decision-making circuit but integrated into it as an active, autonomous, and responsible subject. Under such conditions, automation serves to maintain and strengthen human capabilities rather than replace them. Therefore, a balanced combination of technological efficiency and human control forms the basis for the reliability of emergency adaptive control systems amid the growing dynamism of the digital environment.

Список використаних джерел

1. Амалія Н.Р., Тьяджоно Б., Паладе В. Людина-в-циклі XAI для прогнозного обслуговування: Систематичний огляд інтерактивних систем та їхньої ефективності в прийнятті рішень щодо технічного обслуговування. *Електроніка*, 2025. Вип. 14 (17), С. 3384. DOI: https://doi.org/10.3390/electronics14173384

2. Бейнбрідж Л. Іронія автоматизації. Automatica, 1983Vol. 19, № 6. pp. 775- 779. URL: https://ckrybus.com/static/papers/Bainbridge_1983_Automatica.pdf

3. Вентворт Т. Пояснення ШІ SRE: що це таке, як це працює та реальність людського та ШІ // Incident. URL: https://incident.io/blog/what-is-ai-sre-complete-guide-2026

4. Гонсалес К., Донах'ю К., Гольдштейн Д. Г., Хейдарі Х., Джалалі М. С., Шелбле Б., Сінгх А., Вуллі А. В. На шляху до науки про спільну роботу людини та штучного інтелекту для прийняття рішень: структура взаємодоповнюваності, *PNAS Nexus*, Т. 5, Вип. 3, 2026. DOI: https://doi.org/10.1093/pnasnexus/pgag030

5. Кінцл Я., Адам М. Т., Павлеська Т. Роль людського фактору в управлінні інцидентами кібербезпеки // HCI для кібербезпеки, конфіденційності та довіри. 2025. DOI: 10.1007/978-3-031-92833-8_3

6. Лі Дж. Д., Сеппельт Б. Д. Людський фактор у проектуванні автоматизації // Довідник Springer з автоматизації. Видавництво: Springer Berlin Heidelberg, Берлін, Гейдельберг. 2009. DOI: 10.1007/978-3-540-78831-7_25

7. Лопушняк Г., Поплавська О., Данилевич Н., Костишина Т., Раупов Р. Організація праці в умовах невизначеності: випадок України. *Проблеми та перспективи в менеджменті*, 2023. *21* (2), 294-308. DOI: 10.21511/ppm.21(2).2023.30

8. Лю Юнг-Хуан Нестабільність систем штучного інтелекту та трансформація професійної роботи: наслідки для навичок, ролей та організаційної структури. URL: https://medium.com/@gwrx2005/the-instability-of-artificial-intelligence-systems-and-the-transformation-of-professional-work-ebd035b4fe86

9. Озарко К.С., Піх М.З. Проблеми та перспективи оцінювання інформаційної безпеки підприємств за динамічних умов господарювання. *Економічний вісник Донбасу*. № 3 (81), 2025. С. 208-213. DOI: https://doi.org/10.12958/1817-3772-2025-3(81)-208-213

10. Рейнболт М. Іронія агентного ШІ. URL: https://matthewreinbold.com/2025/03/13/IroniesOfAgenticAI

11. Трім К. Іронія автоматизації. https://medium.com/@craigtrim/the-ironies-of-automation-0f302343bf7d

12. Garcia-Peinado R. Educational Artificial Intelligence, Child Rights, and Human Care in Early Childhood. The European Educational Researcher. DOI: https://doi.org/10.31757/euer.833

13. Paparasuraman R. K., Riley V., Humans and Automation: Use, Misuse, Disuse, Abuse. Honeywell Technology Center, Minneapolis, Minnesota HUMAN FACTORS, 1997, 39(2), 230-253. URL: https://web.mit.edu/16.459/www/parasuraman.pdf

14. Strauch B. Ironies of Automation: Still Unresolved After All These Years. *Ieee Transactions on Human-Machine Systems.* 2017. URL: https://www.jurispro.com/files/articles/roniesofutomationtillnresolvedfterllheseears_4830.pdf

15. Freeman C. Technology policy and economic performance. Frances Printer Publishers, London, New York, 1987. 155 p.